Ako moderná logika vyriešila problémy s pravdivosťou výrokov

Ján Mazák

6. septembra 2024

Čo je výrok? *Oznamovacia veta*,

- ktorá má pravdivostnú hodnotu.
- ktorej sa dá priradiť pravdivostná hodnota.
- pre ktorú má zmysel otázka na jej platnosť, správnosť, pravdivosť.

Nech x je kladné reálne číslo. Potom $x^2 > 0$.

Predstavme si, že p, q sú výroky.

- Je „p or not p“ výrok?
- Je „p or not q“ výrok?

Ako definovať *jednoduchý výrok*? „Neobsahuje logické spojky."

- x delí y
- existuje číslo k také, že k je prirodzené a $y = kx$

Hovoríme to isté, lenže raz s logickou spojkou a raz bez. Pritom ak chceme uchopiť zložitosť výrokov, treba aspoň vedieť určiť, ktoré sú tie najjednoduchšie.

Mimo Zeme žijú niekdajší obyvatelia Atlantídy.

Počet hviez je nepárny.

Zajtra bude pršať.

Zajtra bude pršať.

Odteraz až navždy bude každý deň pršať.

Každé párne číslo je súčtom dvoch prvočísel.
(Goldbachova hypotéza)

Postupnosť $0, 1, 2, 3, 4, 5, 6, \ldots$ je rastúca.

- Je to výrok?

Postupnosť $0, 1, 2, 3, 4, 5, 6, \ldots$ je rastúca.

- Je to výrok?
- Ako vieme, ako bude postupnosť pokračovať?

Postupnosť $0, 1, 2, 3, 4, 5, 6, \ldots$ je rastúca.

- Je to výrok?
- Ako vieme, ako bude postupnosť pokračovať?
- Aký je význam troch bodiek ako symbolu? Môže byť súčasťou výroku popis algoritmu?

Postupnosť $0, 1, 2, 3, 4, 5, 6, \ldots$ je rastúca.

- Je to výrok?
- Ako vieme, ako bude postupnosť pokračovať?
- Aký je význam troch bodiek ako symbolu? Môže byť súčasťou výroku popis algoritmu?
- Môže byť výrok nekonečne dlhý?

Bu bayonot emas.

- Znamená „toto nie je výrok“ v uzbečtine. Aký jazyk je prípustný?

Bu bayonot emas.

- Znamená „toto nie je výrok“ v uzbečtine. Aký jazyk je prípustný?
- Môže výrok hovoriť o sebe?
- Môže viesť k paradoxom: Zoberme množinu X všetkých množín, ktoré neobsahujú samé seba. Je veta „X patrí do X“ výrok? Nemôže to byť ani pravda, ani nepravda, pritom to vyzerá ako úplne korektné matematické vyjadrenie.

Sumarizácia problémov

- Pravdivosť je veľmi ťažké uchopiť.
- Výrok v sebe nesie odkazy na reálny svet, ktoré nesúvisia s logikou a ťažko sa vyhodnocujú.
- Potrebujeme nejaké obmedzenia na použité symboly a ich prípustné kombinovanie.

Riešenie

Definovať výroky tak, aby

- sme sa vyhli pojmu pravdivosti (a pravdivosť výroku definujeme až následne, keď budeme vedieť, čo výrok je);

Riešenie

Definovať výroky tak, aby

- sme sa vyhli pojmu pravdivosti (a pravdivosť výroku definujeme až následne, keď budeme vedieť, čo výrok je);
- logická štruktúra výroku (spojky, kvantifikátory) bola oddelená od sveta, ktorý výrok popisuje;

Riešenie

Definovať výroky tak, aby

- sme sa vyhli pojmu pravdivosti (a pravdivosť výroku definujeme až následne, keď budeme vedieť, čo výrok je);
- logická štruktúra výroku (spojky, kvantifikátory) bola oddelená od sveta, ktorý výrok popisuje;
- symboly, z ktorých výrok pozostáva, patrili do nejakej fixnej abecedy a ich použitie podliehalo jasným syntaktickým/gramatickým pravidlám.

Jazyk logiky

Konštanty zastupujú konkrétne objekty popisovaného sveta.

Jazyk logiky

Konštanty zastupujú konkrétne objekty popisovaného sveta.

Predikáty zastupujú nejaké vlastnosti popisovaného sveta, logike je úplne jedno, aké vlastnosti to sú.

Jazyk logiky

Formula — postupnosť symbolov s jasne danými pravidlami (dobre uzátvorkovaná, logické spojky majú správny počet operandov, za kvantifikátorom nasleduje premenná atď.).

Jazyk logiky

Formula — postupnosť symbolov s jasne danými pravidlami (dobre uzátvorkovaná, logické spojky majú správny počet operandov, za kvantifikátorom nasleduje premenná atď.).
Príklady formúl:

- $0 = 1$
- $\forall x(x \neq 0 \implies x = 1)$
- $\forall x \exists y[P(x) \wedge Q(x, y)]$
- $P(x) \implies \neg Q(7)$
  — tzv. otvorená formula, zodpovedá výrokovej forme

Logika zrazu nie je len jedna — jednotlivé logické jazyky sa líšia o.i. v konštantách, môžeme tiež obmedziť použitie logických spojok.

Chceme vedieť algoritmicky rozhodovať o tom, ktorá postupnosť symbolov je formula?

Pravdivosť formúl

Je P(alf) pravda?

Aby bolo možné skúmať pravdivosť, treba pridať intepretácie pre všetky mimologické symboly.

Pravdivosť formúl

- Konštanty budú prvky nejakej množiny D (doména).

Pravdivosť formúl

- Konštanty budú prvky nejakej množiny D (doména).
- Predikát je pravdivý pre niektoré prvky z D (podmnožina domény).

Pravdivosť formúl

- Konštanty budú prvky nejakej množiny D (doména).
- Predikát je pravdivý pre niektoré prvky z D (podmnožina domény).
- Kvantifikované premenné nadobúdajú hodnoty z domény: $\exists x P(x)$ vyjadruje, že v D sa nachádza prvok d, pre ktorý platí $P(d)$.

Pravdivosť formúl

- Konštanty budú prvky nejakej množiny D (doména).
- Predikát je pravdivý pre niektoré prvky z D (podmnožina domény).
- Kvantifikované premenné nadobúdajú hodnoty z domény: $\exists x P(x)$ vyjadruje, že v D sa nachádza prvok d, pre ktorý platí $P(d)$.

Úloha: uvažujme formulu $\forall x(x = c_0 \vee x = c_1)$.
Nájdite doménu a interpretáciu konštánt, pre ktoré je táto formula (a) pravdivá, (b) nepravdivá.

Načo je to dobré? Databázy

Bežná databáza obsahuje tabuľky, v ktorých sú zoznamy objektov spĺňajúcich predikáty. Napr. tabuľka s dvojicami (meno, rodné číslo) popisuje predikát s dvomi argumentmi. Databázy sa potom pýtame otázky v podobe „nájdi mi všetky x, ktoré spĺňajú nejakú formulu vyjadrujúcu požadovanú vlastnosť x“. Napr. „rodné čísla ľudí, ktorí sa volajú Jozef“.

Načo je to dobré? Databázy

Pri návrhu databázového systému potrebujeme presne popísať, aké formuly je povolené použiť v dotazoch. Čím zložitejšie formuly, tým viac nimi možno vyjadriť, ale zároveň sa ťažšie vyhodnocujú. Aj preto sa dotazy píšu v špeciálnych jazykoch ako SQL, nie v C či Pythone.

Pravdivosť formúl

Podarilo sa nám oddeliť vlastnosť „byť formulou“ od pravdivosti. Jedna formula môže byť pravdivá i nepravdivá, závisí od interpretácie mimologických symbolov.

Množine formúl hovoríme teória. Teória tiež môže byť pravdivá i nepravdivá. Interpretáciám, v ktorých je teória pravdivá, hovoríme model.

Pravdivosť formúl

Zväčša nás nezaujíma vymýšľanie interpretácií, ale vzťahy medzi formulami — logické vyplývanie. Typická otázka je, či z teórie T vyplýva formula F. Napr. keď ako teóriu T vezmeme aritmetiku a pýtame sa, či z T vyplýva „súčet dvoch prvočísel je vždy párny“.

Toto sa dá úplne presne definovať: je pravda, že každý model T je modelom F?
Je pravda, že v každom svete, v ktorom sú splnené všetky formuly z T, je splnená aj F?

Úloha: Nech A, B sú formuly.
Je pravda, že z $A \vee \neg B$ a B vyplýva A?

Čo je to dôkaz?

Kľúčová idea: dokazovacie systémy sú mechanické, algoritmické, realizovateľné na počítači bez akýchkoľvek úvah o tom, čo je pravda či pre ktoré interpretácie je formula pravdivá.
Korektnosť a úplnosť.

Čo je to dôkaz?

Kľúčová idea: dokazovacie systémy sú mechanické, algoritmické, realizovateľné na počítači bez akýchkoľvek úvah o tom, čo je pravda či pre ktoré interpretácie je formula pravdivá.

Hilbertov program (1900): nájdime takú sadu axióm (teóriu), že pre každú matem. formulu F možno dokázať F alebo $\neg F$.

Čosi podobne sa podarilo Euklidovi s planimetriou: na základe 5 axióm (v skutočnosti asi 20) dokázal platnosť všetkých podstatných planimetrickych tvrdení známych Grékom.

Gödelova veta o neúplnosti (1930)

Nemožno axiomatizovať ani len aritmetiku. Presnejšie, nemožno nájsť teóriu T, ktorá má zároveň nasledujúce vlastnosti:

- T je prvého rádu a je korektná [ak nie, pravdivosť nebude totožná s dokázateľnosťou],
- z T nevyplýva nepravda [ak by vyplývala, tak z tejto nepravdy už vyplýva čokoľvek, čiže T je nanič],
- T je efektívne axiomatizovateľná [ak by nie, nevieme algoritmicky ani len rozhodnúť, čo je formula či dôkaz],
- T obsahuje aritmetiku (sčítanie, násobenie, prirodzené čísla),
- T je negačne úplná (pre každú formulu vyjadriteľnú v jazyku T máme jej dôkaz alebo vyvrátenie).

Čomu sa venuje logika dnes?

- zúženia prvorádovej logiky (napr. monadická), logika vyššieho rádu
- rôzne výpočtové aspekty (automatické dokazovače, SAT solvery, zložitosť problémov)
- fuzzy logika, modálne logiky (reprezentácia „možno“/„morálne akceptovateľné“/...)
- mnoho teoretických tém, ktorým nerozumiem